AD-A033 377 MASSACHUSETTS UNIV AMHERST DEPT OF ELECTRICAL AND C--ETC F/G 9/4
APPLICATIONS OF INFORMATION AND SYSTEM THEORY TO AIR FORCE PROB--ETC(U)
OCT 76 J K WOLF

UNCLASSIFIED

AF-AFOSR-2601-74

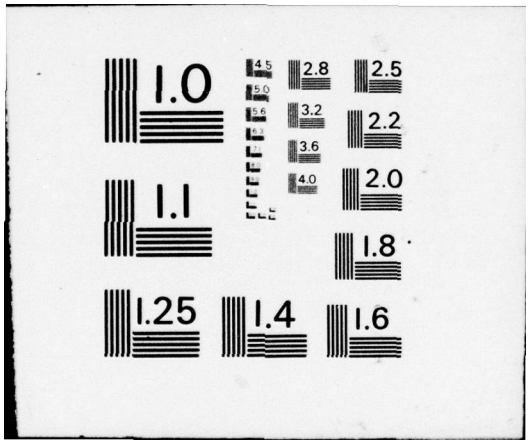
AFOSR-TR-76-1234

NL

1 OF 1
ADA033377

END

DATE
FILMED
2 - 77


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6

AFOSR - TR - 76 - 1234

3

Communications and Systems

Electrical and Computer Engineering

University of Massachusetts
at Amherst

4. TITLE (and Subtitle)
APPLICATIONS OF INFORMATION AND SYSTEM THEORY TO AIR FORCE PROBLEMS IN COMMUNICATIONS AND DATA HANDLING

5. TYPE OF REPORT & PERIOD COVERED
Interim

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
J. K. Wolf

8. CONTRACT OR GRANT NUMBER(s)
AFOSR 74-2601
405 589

9. PERFORMING ORGANIZATION NAME AND ADDRESS
University of Massachusetts
Dept of Electrical & Computer Engineering
Amherst, MA 01003

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
2304/A6
61102F

11. CONTROLLING OFFICE NAME AND ADDRESS
Air Force Office of Scientific Research/NM
Bolling AFB, DC 20332

12. REPORT DATE
15 Oct 76

13. NUMBER OF PAGES
25

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)
This report summarizes the results of research performed under Grant AFOSR 74-2601 for the period 1 Sep 75 to 31 Aug 76. The research was concerned with problems in communications theory and information theory and their application. Specific problems considered were: (a) soft decision decoding of linear block codes. (b) application of coding to computers (c) coding for noisy channels including multi-user channels.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER: AFOSR - TR - 76 - 1234	2. GOVT ACCESSION NO. / 3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle): APPLICATIONS OF INFORMATION AND SYSTEM THEORY TO AIR FORCE PROBLEMS IN COMMUNICATIONS AND DATA HANDLING	5. TYPE OF REPORT & PERIOD COVERED: Interim
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): J. K. Wolf	8. CONTRACT OR GRANT NUMBER(s): AFOSR 74-2601
9. PERFORMING ORGANIZATION NAME AND ADDRESS: University of Massachusetts, Dept of Electrical & Computer Engineering, Amherst, MA 01003	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: 2304/A6, 61102F
11. CONTROLLING OFFICE NAME AND ADDRESS: Air Force Office of Scientific Research/NM, Bolling AFB, DC 20332	12. REPORT DATE: 15 Oct 76
	13. NUMBER OF PAGES: 25
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)	15. SECURITY CLASS. (of this report): UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)
This report summarizes the results of research performed under Grant AFOSR 74-2601 for the period 1 Sep 75 to 31 Aug 76. The research was concerned with problems in communications theory and information theory and their application. Specific problems considered were: (a) soft decision decoding of linear block codes. (b) application of coding to computers (c) coding for noisy channels including multi-user channels.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

(16) 2304 (18) AFOSR

(15) AF-AFOSR-2601-74 (17) A6 (19) TR-76-1234

ASOFR-74-2601

(11) 15 October 15, 1976

(12) 31p.

(9) Interim Scientific Report.
1 Sep 75 - 31 Aug 76

(6) Applications of Information and System Theory to Air Force Problems in Communications and Data Handling.

Principal Investigator (10) J. K. Wolf

Prepared under Grant AFOSR-74-2601

Report for period

September 1, 1975 to August 31, 1976

Department of Electrical and Computer Engineering

University of Massachusetts

Amherst, Massachusetts 01003

Sponsored by

Air Force Office of Scientific Research
Air Force Systems Command, USAF
1400 Wilson Boulevard
Arlington, Va. 22209

Approved for public release;
distribution unlimited.

1473

405 589 AB

Abstract

This report summarizes the results of research performed under Grant AFOSR-74-2601 for the period September 1, 1975 to August 31, 1976. The research was concerned with problems in communications theory and information theory and their applications. Specific problems considered were:

(a) Soft decision decoding of linear block codes.

(b) Application of coding to computers.

(c) Coding for noisy channels including multi-user channels.

Table of Contents

I. Introduction

This is an interim technical report under Grant AFOSR-74-2601 sponsored by the Air Force Office of Scientific Research for the period September 1, 1975 to August 31, 1976. Two previous interim reports, one issued in September 1974, and the other issued in October 1975, covered the work conducted during the first two years of this grant, September 1, 1973 to August 31, 1975. This work was conducted at the University of Massachusetts, Amherst, Massachusetts. It is a follow-on to research previously conducted at the Polytechnic Institute of Brooklyn.

The research performed under this contract was primarily concerned with problems in communications theory and information theory. Specific problems considered were soft decision decoding for linear block codes, applications of coding to computers, and coding for noisy channels including multi-user channels.

In Section II, a brief summary of the research activity for the grant period is presented. The details of this research are contained in the published papers.

Section III contains a list of such papers plus symposia and invited talks concerned with research conducted under this grant. Section IV mentions an award presented to the principal investigator for a paper on previous research on multi-user communications. Finally Sections V and VI contain titles of dissertations and journal articles on research supported by previous AFOSR contracts and grants.

II. Summary of Research

1. Soft Decision Decoding for Linear Block Codes

A new method has been found for achieving maximum likelihood detection of the q^k code words in a (n,k) linear block code with symbols from GF(q). This method can utilize soft decisions (i.e. analog signals) as well as hard decisions. For an additive channel where the noise in each signalling interval is independent of all other signalling intervals, the complexity of the decoder when using either soft or hard decisions is proportional to q^{n-k} (or sometimes q^{ℓ} where $\ell < n-k$). The method is analogous to the use of the Viterbi algorithm[1] for convolutional codes.

To compare this method with conventional word decoding, consider a (31,26) binary code. Word correlation requires comparing the received waveform with 2^{26} distinct code words. The method referred to above required storing no more than 2^5 quantities at any time.

Rather than explain the method in general, we consider here only a cyclic (15,11) binary Hamming code. The details of the generalization to nonbinary, noncyclic, codes is covered in a paper which has been prepared on this subject.

Example Decoding a (15,11) Binary Cyclic Code

Consider the (15,11) binary cyclic code with generator polynomial $g(x) = x^4 + x + 1$. One method of forming the code words for this code is via the encoding circuitry shown in Figure 1.

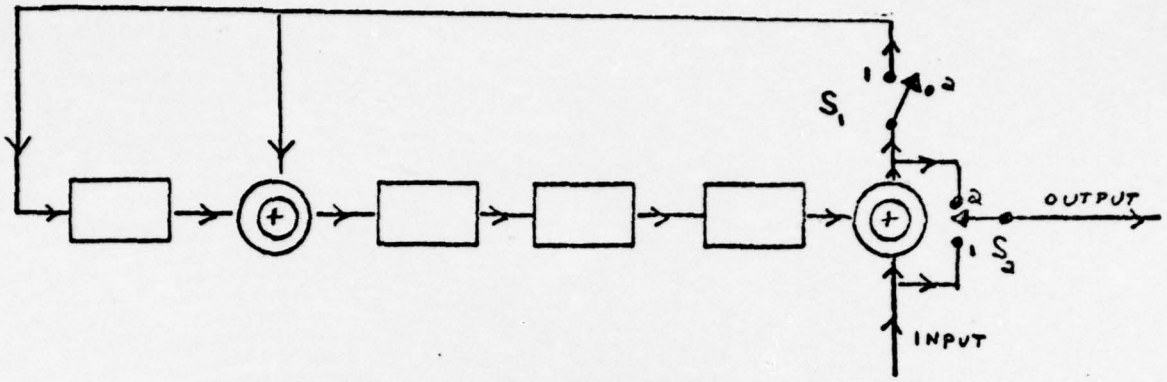


Figure 1. Encoder for code with n=15, k=11, and r=4

For the first 11 clock pulses, switches S_1 and S_2 are in position 1 and the input consists of the 11 message digits. For the next 4 clock pulses, switches S_1 and S_2 are in position 2 and zeros are fed in at the input. The first 11 digits which appear at the output are then the 11 message digits and the last 4 digits which appear at the output are the 4 check digits. As an example we show the operation of this circuit if the message digits are 1 0 1 0 0 1 0 1 1 1 0.

	← State of Encoder →				
input	1st flip flop	2nd flip flop	3rd flip flop	4th flip flop	output
	0	0	0	0	
1	1	1	0	0	1
0	0	1	1	0	0
1	1	1	1	1	1
0	1	0	1	1	0
0	1	0	0	1	0
1	0	1	0	0	1
0	0	0	1	0	0
1	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	1
0	1	0	1	1	0
0	0	1	0	1	1
0	0	0	1	0	1
0	0	0	0	1	0
0	0	0	0	0	1

The state sequence for the encoder for this input is then

0 0 0 0 → 1 1 0 0 → 0 1 1 0 → 1 1 1 1 → 1 0 1 1 → 1 0 0 1 → 0 1 0 0 → 0 0 1 0 →
1 1 0 1 → 0 1 1 0 → 1 1 1 1 → 1 0 0 1 → 0 1 0 1 → 0 0 1 0 → 0 0 0 1 → 0 0 0 0

We now form what is known as the trellis diagram for this code. Prior to a message digit entering the encoder, the encoder contains the digits 0 0 0 0 in its four flip flops. We say the encoder is in 0 0 0 0 state. If a 0 enters the encoder as the message digit, the encoder remains in the 0 0 0 0 state while if a 1 enters the encoder, the encoder goes to the 1 1 0 0 state. This is shown in Figure 2. The possible states after

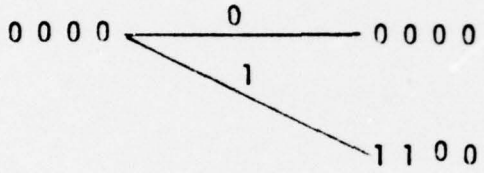


Figure 2. Start of Trellis for Encoder of Figure 1.

2, 3 and 4 message digits are shown in Figure 3. Note that after 4 message digits all 16 possible states are reached by each of the 16 possible message sequences. For the next 7 message digits the trellis does a peculiar thing. Each state is entered from exactly two other states. The trellis for these next 7 message digits is shown in Figure 4. Finally on the 12^{th} through 15^{th} clock pulse, zeros are entered into the encoder and the trellis collapses as shown in Figure 5. The trellis for the complete encoder thus consists of a concatenation of Figure 3, 7 sections of Figure 4 and the end of the trellis as in Figure 5. In every case the branches of the trellis are labeled by 0 or 1 corresponding to the digit of the code word transmitted. A code word is then identified by a path through the trellis from beginning to end where each code word is identified by a unique path. A typical path is shown in Figure 6 corresponding to the code word 1 0 1 0 0 1 0 1 1 1 0 1 0 0 1.

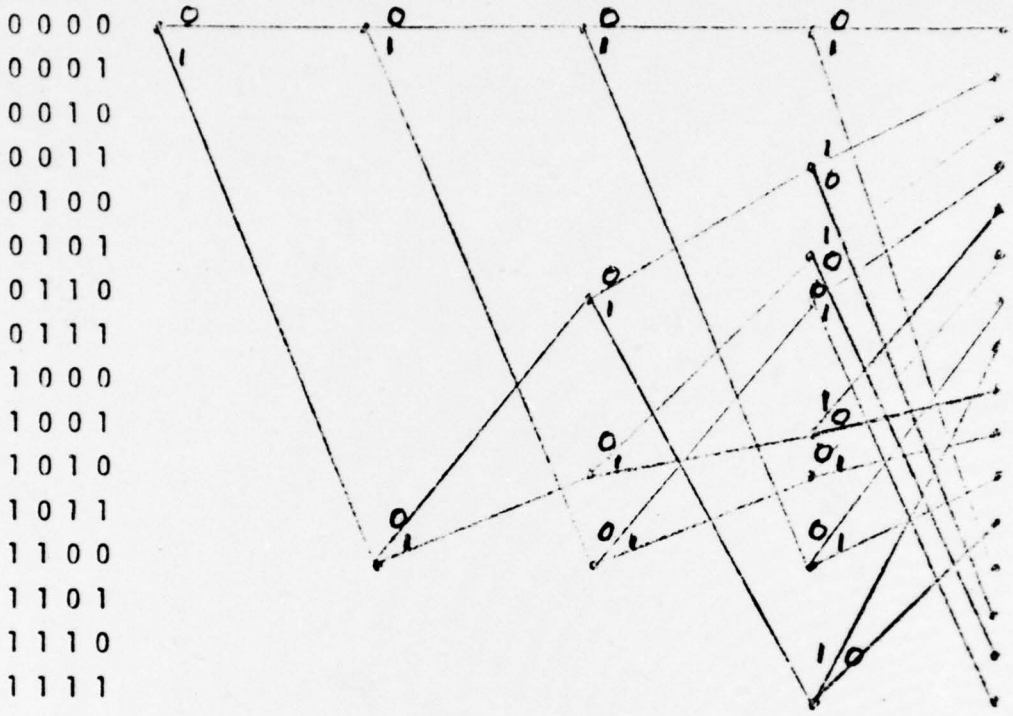


Figure 3. Trellis for up to 4 message digits

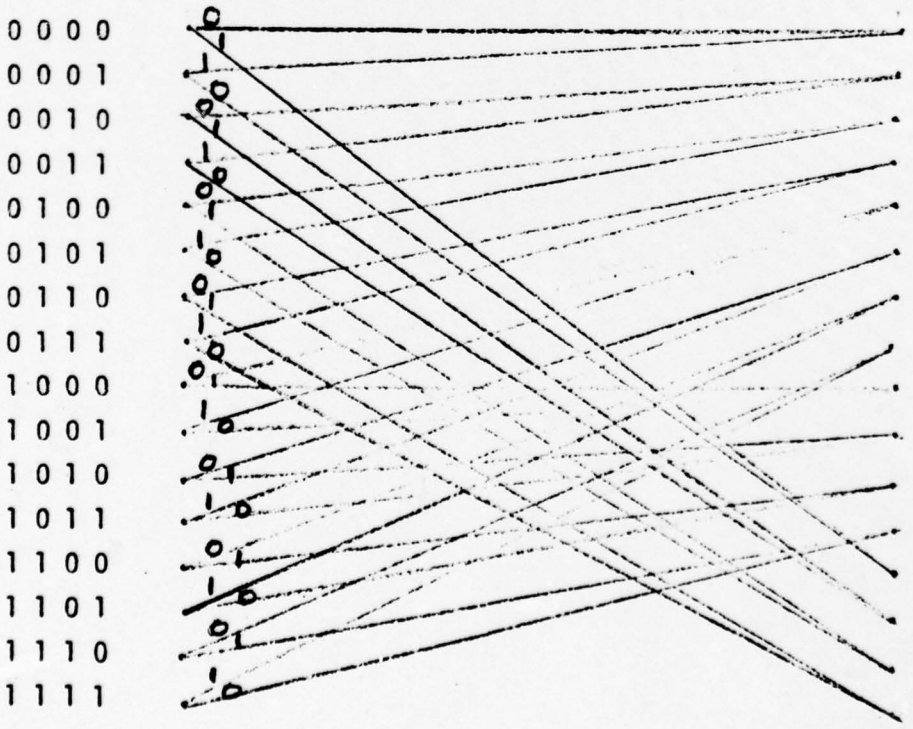


Figure 4. Trellis structure for message digits 5 through 11

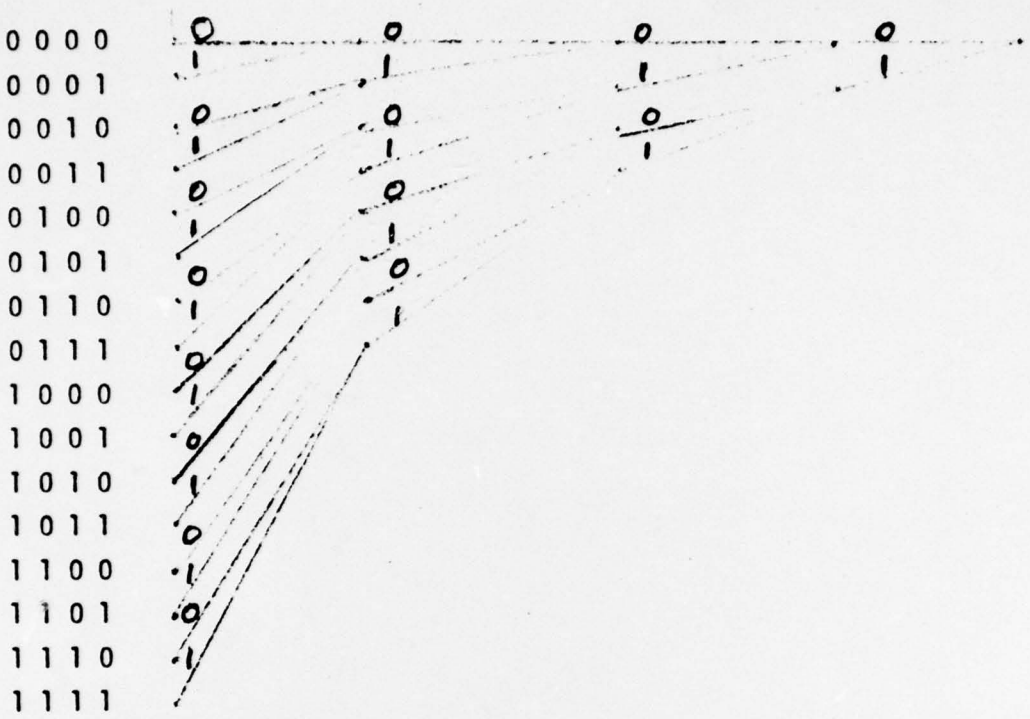


Figure 5. End of Trellis for clock pulses 12 through 15

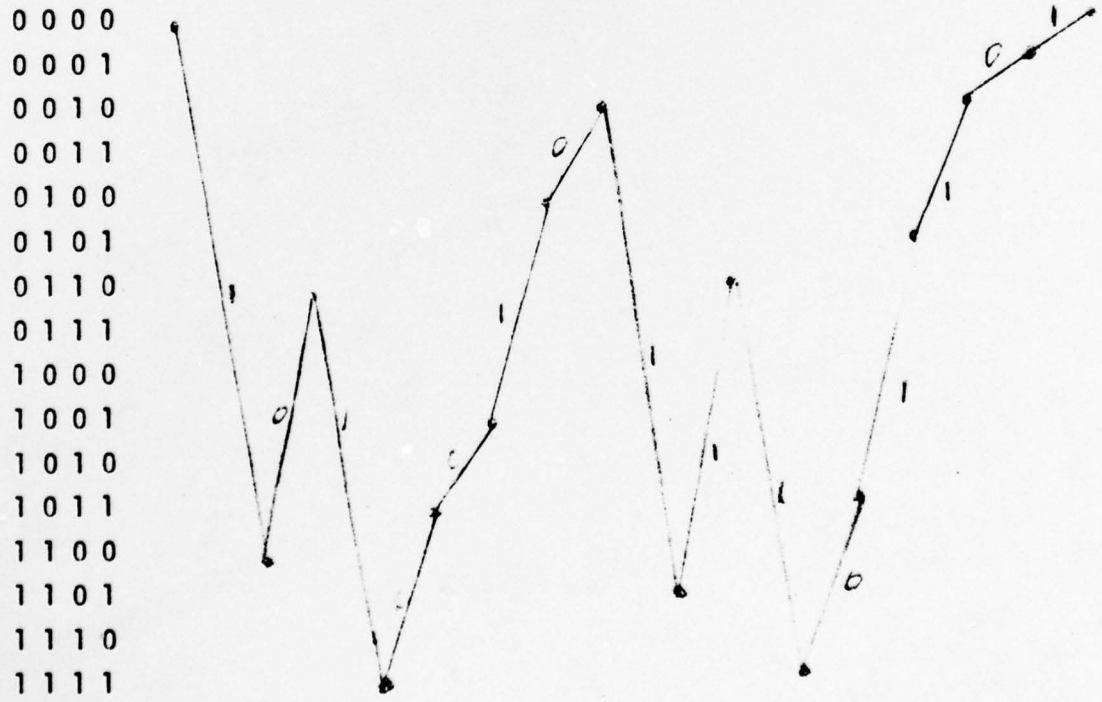
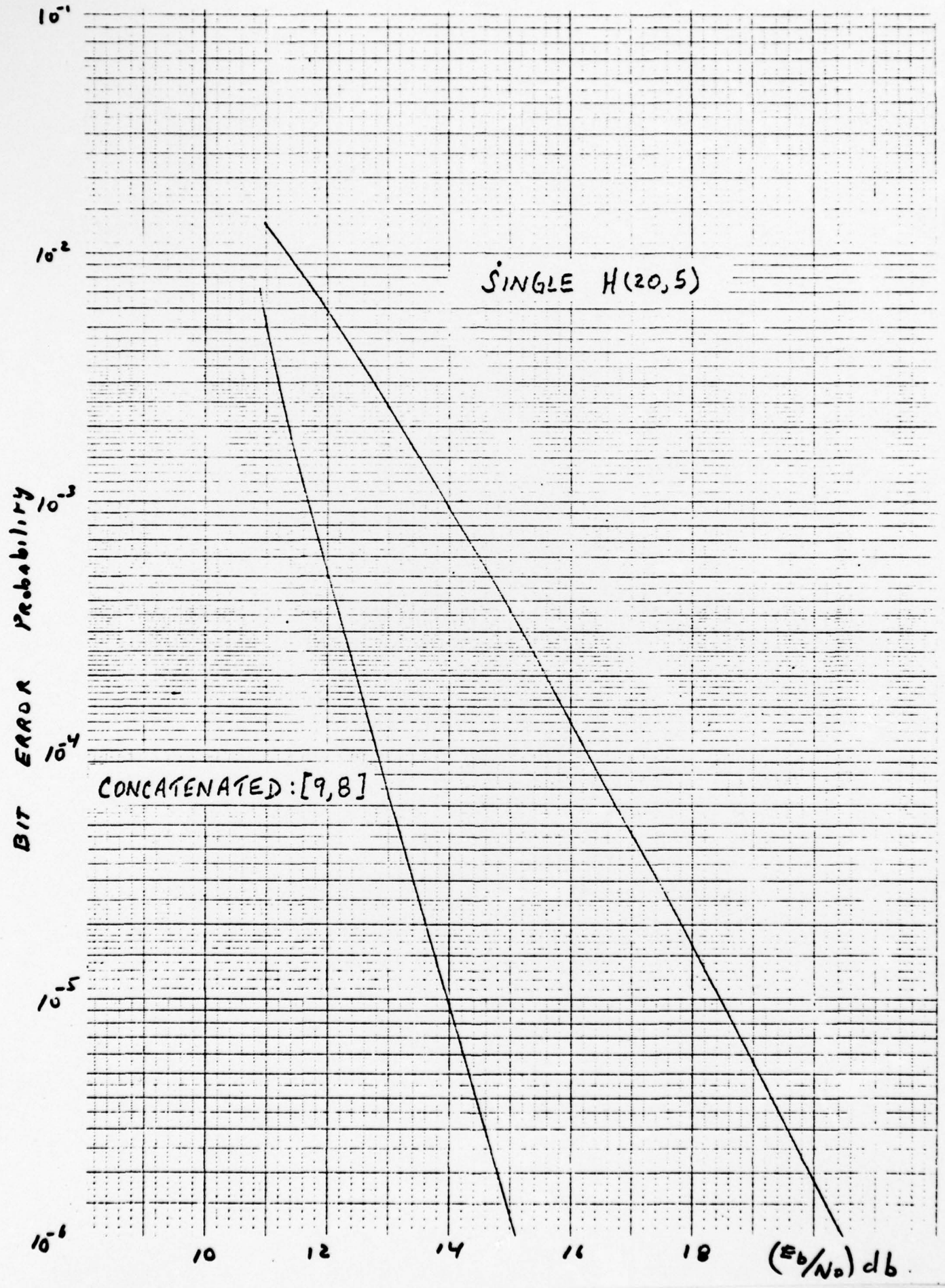


Figure 6. Path in Trellis for Code Word 1 0 1 0 0 1 0 1 1 1 0 1 1 0 1

Once the trellis has been constructed for the code, the Viterbi[1] algorithm can be used to find the maximum likelihood path through the trellis. This algorithm can be used for either a hard decision receiver or a soft decision receiver. (A soft decision receiver is one where channel measurement information is available at the decoder.) However, since we are concerned with a code where a very simple algebraic decoding algorithm is known for hard decisions, it would appear that the technique discussed here would only be of interest in the case of soft decisions.

The use of this technique has been suggested for decoding constant weight binary codes in a particular fading channel. (This is research presently being performed by Stein Associates under Contract N-00140-76-C-6533 for the Naval Underwater Systems Center.) The details of this work are not included here, but rather a pair of curves are shown in Figure 7, giving the bit error probability versus average ratio of the energy per bit to noise power density for two competing systems. The curve labeled "Single H(20,5)" is a coded system previously considered by others. The curve labeled "Concatenated: [9,8]" is a system which uses the techniques developed under this grant. The system has 2^{40} code words and it would have been impossible to consider such a system if one had to consider comparing the received signal with each of the code words.


BIT ERROR Probability
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
SINGLE H(20,5)
CONCATENATED: [9,8]
10
12
14
16
18
(E_b/N_o) db

2. Application of Coding to Computers

A particular application of the Chinese Remainder Theorem to the design of fault tolerant computers has been investigated. A brief summary of this work follows.

The basic theorem to be used is the following: Let $m_1, m_2, \cdots, m_L$ be L positive integers that are relatively prime in pairs. Let "I" be any non-negative integer less than $m = \prod_{i=1}^{L} m_i$. Then "I" can be uniquely reconstructed from its remainders, $r_1, r_2, \cdots, r_L$ where $I = Q_i m_i + r_i$ $0 \leq r_i < m_i$, $i = 1,2,\cdots,L$.

An example is given in the following table for $m_1 = 2$, $m_2 = 3$ and $m_3 = 5$.

I	r_1	r_2	r_3	I	r_1	r_2	r_3
0	0	0	0	15	1	0	0
1	1	1	1	16	0	1	1
2	0	2	2	17	1	2	2
3	1	0	3	18	0	0	3
4	0	1	4	19	1	1	4
5	1	2	0	20	0	2	0
6	0	0	1	21	1	0	1
7	1	1	2	22	0	1	2
8	0	2	3	23	1	2	3
9	1	0	4	24	0	0	4
10	0	1	0	25	1	1	0
11	1	2	1	26	0	2	1
12	0	0	2	27	1	0	2
13	1	1	3	28	0	1	3
14	0	2	4	29	1	2	4

An important corollary to this theorem is:

Let S be a subset of the integers $m_1, m_2, \cdots m_L$. If I is an integer in the range $0 \leq I < \prod_{i=S} m_i$, then I can be uniquely reconstructed from the remainders corresponding to the m_i in this subset.

To see that this is the case consider the previous example where $m_1 = 2$, $m_2 = 3$, $m_3 = 5$. Then we can consider three sets S as follows:

$S_1 = \{m_1, m_2\}$			$S_2 = \{m_1, m_3\}$			$S_3 = \{m_2, m_3\}$		
I	r_1	r_2	I	r_1	r_3	I	r_2	r_3
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
2	0	2	2	0	2	2	2	2
3	1	0	3	1	3	3	0	3
4	0	1	4	0	4	4	1	4
5	1	2	5	1	0	5	2	0
			.			.		
			.			.		
			.			.		
			9	1	4	14	2	4

Thus given the remainders (r_1, r_2, r_3), any two of these remainders can uniquely determine an integer I in the range $0 \leq I < 5$.

Finally we consider a second corollary to the Chinese Remainder Theorem:

Let I be a non-negative integer in the range $0 \leq I < M$. Let $m_1 < m_2 < \cdots < m_N$ be positive integers that are relatively prime in pairs. Let s be the smallest integer such that $\prod_{i=1}^{s} m_i \geq M$. Then "I" can be uniquely determined from any s remainders from the set $\{r_1, r_2, \cdots, r_N\}$.

Let s and N be defined as in the previous corollary. Consider the set of remainders $r_1, r_2, \cdots, r_N$ where now F of these remainders are erased (i.e. are missing) and T of them are in error. Assume that $2T + F \leq N - s$. Then one can uniquely determine I from the remaining N-F unerased remainders, T of which are in error.

As an example, let

$$m_1 = 97,\ m_2 = 101,\ m_3 = 103,\ m_4 = 107 \text{ and } m_5 = 109.$$

Then if $0 \leq I < 97 \cdot 101 = 9797$, $s = 2$, $N = 5$ and $N-s = 3$. Then I can be reconstructed if

(a) one remainder was in error,

or

(b) two or one remainder are erased.

We now apply these ideas to fault tolerant computers.

Let I_1 and I_2 be two integers in the range $0 \leq I_1, I_2 < m = m_1 m_2 \cdots m_N$. Then if I_1 and I_2 have the remainders

$$I_1 \rightarrow (r_{11}, r_{12}, \cdots, r_{1N}),$$

and

$$I_2 \rightarrow (r_{21}, r_{22}, \cdots, r_{2N}),$$

then

$$(I_1 \pm I_2)_m = ((r_{11} \pm r_{21})_{m_1}, (r_{12} \pm r_{22})_{m_2}, \ldots, (r_{1N} \pm r_{2N})_{m_N})$$

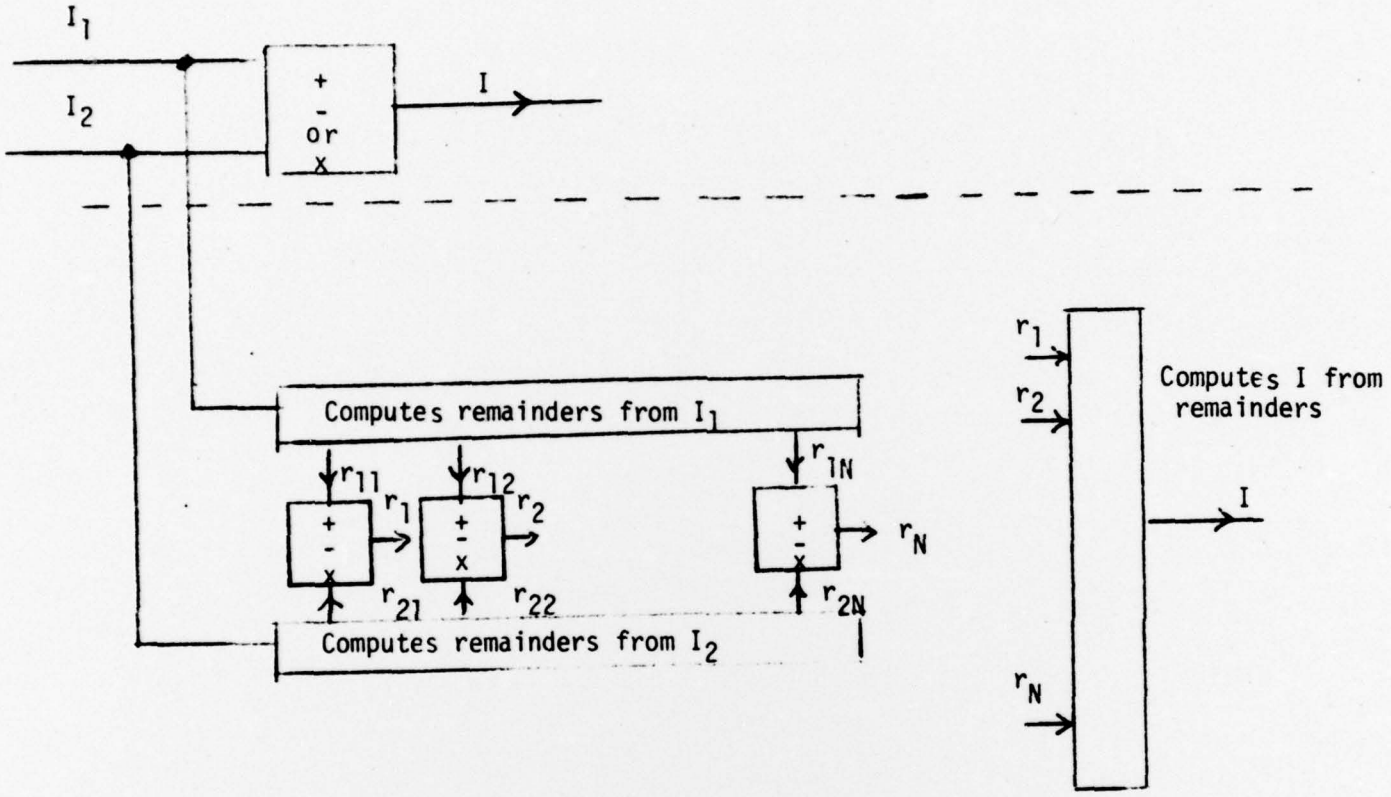
and

$$(I_1 \cdot I_2)_m\ ((r_{11} \cdot r_{21})_{m_1}, (r_{12} \cdot r_{22})_{m_2}, \cdots (r_{1N} \cdot r_{2N})_{m_N})$$

where $(x)_y$ means x mod y.

This result has been previously suggested for use in a residue number system computer. The advantage of such a computer is that addition and multiplication can be very fast. A disadvantage is that it is difficult to compare the magnitude of I_1 and I_2 from their remainders. We will be interested in considering a fault-tolerant residue number system computer. Let $m_1 < m_2 < \cdots < m_N$ be pairwise prime, and let $0 \leq I_1, I_2 < M = m_1 m_2 \cdots m_s$.

Consider the two systems shown below where $\boxed{\begin{smallmatrix}+\\-\\\text{or}\\\times\end{smallmatrix}}$ is a box that does addition, subtraction or multiplication (perhaps modulo some integer).



From the previous discussion we see that the system below the dotted line will work if T $\boxed{\begin{smallmatrix}+\\-\\\times\end{smallmatrix}}$'s produce faulty outputs and F produce no outputs at all where

$$2T + F \leq N\text{-}s.$$

The system above the dotted line is the non-fault-tolerant version of the system.

Note that one can tolerate twice as many failed $\boxed{\begin{smallmatrix}+\\-\\\times\end{smallmatrix}}$'s as $\boxed{\begin{smallmatrix}+\\-\\\times\end{smallmatrix}}$'s that produce errors.

Thus one can use an error detection code to convert errors in these boxes into erasures. One such code that will detect any single carry or sum error in an adder is to multiply each remainder by 3. Thus we would go through the following steps.

a. $I_1 \rightarrow (r_{11}, r_{12}, \cdots, r_{1N})$

$I_2 \rightarrow (r_{21}, r_{22}, \cdots, r_{2N})$

↑ Encode ↓

b. $(r_{11}, r_{12}, \cdots, r_{1N}) \longrightarrow (3r_{11}, 3r_{12}, \cdots, 3r_{1N})$

$(r_{21}, r_{22}, \cdots, r_{2N}) \longrightarrow (3r_{21}, 3r_{22}, \cdots, 3r_{2N})$

c. Form $(3r_{11} + 3r_{21})_{3m_1} \rightarrow a_1$

$(3r_{12} + 3r_{22})_{3m_2} \rightarrow a_2$

↑ Addition ↓ Actual results may contain errors

$\vdots$

$(3r_{1N} + 3r_{2N})_{3m_N} \rightarrow a_N$

↑ Decode

d. Calculate $(a_1)_3 \; (a_2)_3 \cdots (a_N)_3$

If $(a_i)_3 \neq 0$ replace a_i by $\emptyset$ (null symbol). Otherwise let a_i alone. Call result $(\hat{a}_1, \hat{a}_2, \cdots, \hat{a}_N)$

↓ Decode

where $\hat{a}_i = \begin{cases} \emptyset & (a_i)_3 \neq 0 \\ \frac{a_i}{3} & (a_i)_3 = 0 \end{cases}$

e. Reconstruct $I_1 + I_2$ from $(\hat{a}_1, \hat{a}_2, \cdots, \hat{a}_N)$

The procedure will work if

(No of $\emptyset$'s) + 2 (No of incorrect $\hat{a}_i$) $\leq$ N-s.

3. Coding for Noisy Channels Including Multi-User Channels

We have considered various schemes for coding for multi-user communication channels. One such channel is discussed here—the modulo 2 channel.

We consider a multiple access channel where two users must separately encode information for a common channel. We assume word and bit synchronization for the encoders but that they are unaware of the information to be transmitted by the other user. The channel to be considered is a channel which accepts a pair of binary symbols and produces as its output a binary symbol which is the modulo 2 summation of the input symbols.

Let R_1 and R_2 be the rates of the two users (in bits per channel use). It is well known that the capacity region of the modulo 2 channel is given by the equation

$$0 \leq R_1 + R_2 \leq 1.$$

Furthermore any point on the line $R_1 + R_2 = 1$ can be achieved by time sharing between two modes of operation where in each mode one encoder transmits uncoded data and the other encoder transmits all zeros.

An alternative scheme exists for achieving the rate pair $(R_1,R_2) = (\frac{k}{N}, 1 - \frac{k}{N})$. An (N,k) binary cyclic code is chosen as the code for encoder 1. This code has generator polynomial g(x) and parity check polynomial h(x). It is assumed that N is an odd integer so that g(x) and h(x) have no common factors.

Let encoder 1 transmit a code word from the (N,k) binary code and let encoder 2 transmit a code word from the (N,N-k) dual code with generator polynomial h(x). Let $I_1(x)$ be the idempotent for the (N,k) code and let $I_2(x) = 1 \oplus I_1(x)$ be the idempotent for the dual code.

The decoder then receives a word of the form

$$a(x)g(x) \oplus b(x)\, h(x).$$

To obtain the code word transmitted by encoder 1, it multiplies by $I_1(x)$, modulo X^N-1. To obtain the code word transmitted by encoder 2, it multiplies by $I_2(x)$, modulo X^N-1.

This scheme is a special case of the following: Encoder 1 transmits a word from an (N,k) binary code. A coset table is formed where the coset leaders form an (N,N-k) binary group code. The receiver receives a word in the coset table, say in the i^{th} row and j^{th} column. It then decodes to the j^{th} code word used by encoder 1 and the i^{th} code word used by encoder 2.

The advantage of this scheme over simple time sharing will be discussed when we consider the modulo 2 channel with errors.

Modulo 2 Channel With Errors

Let us consider a modulo 2 channel with errors as the cascade of the modulo 2 channel without errors and a binary symmetric channel with cross-over probability p. The capacity region for this channel is given by the equation

$$0 \leq R_1 + R_2 \leq 1 - h(p)$$

where h(p) is the entropy function.

One approach to coding for such a channel is to time share between two modes of operation where in one mode one encoder uses a t error correcting code (say a BCH code) while the other encoder sends all zeros. In the other mode the encoders switch roles.

Another approach is as follows: Let g(x) be the generator polynomial of a binary cyclic code which corrects t errors. Let $X^N-1 = g(x)h_1(x)h_2(x)$ where N is odd so that g(x), $h_1(x)$ and $h_2(x)$ have no common factors. Let encoder 1 use code words from a cyclic code with generator polynomial $g(x)h_1(x)$ while encoder 2 uses code words from a cyclic code with generator polynomial $g(x)h_2(x)$.

The received word is of the form

$$a(x)g(x)h_1(x) \oplus b(x)g(x)h_2(x) \oplus n(x) = \alpha(x)g(x) \oplus n(x)$$

The received word can be decoded correctly to $\alpha(x)g(x)$ if no more than t errors occurred in $n(x)$. Then one can find $a(x)$ and $b(x)$ by using the idempotents of the codes with generators $g(x)h_1(x)$ and $g(x)h_2(x)$.

The advantage of this scheme over time sharing is that if one source is not transmitting (i.e., the encoder is transmitting all zeros) the error correction capability of the code increases. For example, let $N = 63$, $g(x) = m_1(x)m_3(x)m_5(x)m_7(x)$, $h_1(x) = m_9(x)m_{11}(x)m_{13}(x)$ and $h_2(x) = m_{15}(x)$ $m_{23}(x)m_{27}(x)m_{31}(x)$ where $m_i(x)$ is the minimum function of α^i and α is a primitive element of GF(64). Then $g(x)$ is the generator polynomial of a 7 error correcting code, $g(x)h_2(x)$ is the generator polynomial of an 8 error correcting code. Thus if both sources are transmitting, 4 errors can be corrected while if only one source is transmitting the code can correct 7 or 8 errors.

References

1. A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," IEEE Trans. Information Theory, Vol. IT-13, pp. 260-269, April 1967.

III. Papers, Symposia and Invited Talks

1. A series of four papers in the book Information Theory: New Trends and Open Problems, edited by G. Longo, Springer-Verlag, Wien, New York, 1975.
   (a) "The AEP Property of Random Sequences and Applications to Information Theory, Part I: Basic Principles", pp. 125-138.
   (b) "Part II: Single-User Communications", pp. 139-146.
   (c) Part III: Multi-User Communications", pp. 147-156.
   (d) "Constructive Codes for Multi-User Communication Channels", pp. 157-172.
2. "Communication From Several Sources to Several Receivers", presented at URSI Meeting, Boulder, Colorado, October 20-23, 1975.
3. "Coding", presented at Fault Tolerant Systems Workshop sponsored by NASA and USAF Avionics Laboratory, December 3-5, 1975, Research Triangle, Institute, North Carolina.
4. Series of four lectures presented at the Universidad Central de Venezuela at invitation of Consijo de Desarrollo, Cientifico y Humanestico, Caracus, Venezuela, January 20-23, 1976.
   (a) "Reliable Communication in Additive Gaussian White Noise-Uncoded Case".
   (b) "Reliable Communication in Additive Gaussian White Noise-Coded Case".
   (c) "Source Coding and Data Compression".
   (d) "Error Correcting Codes and Fault Tolerant Computation".
5. "Soft Decision Decoding" presented at Workshop on Communication Theory, April 26-28, 1976, Florida.
6. "Decoding of Block Codes Using Reliability Information" presented at Fourth International Symposium on Information Theory, June 15-19, 1976,

Leningrad, USSR (Invited Paper).

7. "Permutation Codes for the Gaussian Broadcast Channel", (with H. de Pedro and C. Heegard) presented at 1976 IEEE International Symposium on Information Theory, Ronneby, Sweden, June 21-24, 1976.
8. A series of lectures presented at Summer School on Information in Large Networks, sponsored by CISM - The International Centre for Mechanical Sciences, Udine, Italy, June 28 to July 9, 1976.
   (a) "Soft Decision Decoding of High Rate Block Codes".
   (b) "Error Control for a Satellite Packet Switching Network".
   (c) "Permutation Codes for the Gaussian Broadcast Channel with Two Receivers".
   (d) "The Chinese Remainder Theorem and Applications".

IV. Awards

Co-recipient with David Slepian of Bell Telephone Laboratories of the Information Theory Group Prize Paper Award for paper "Noiseless Coding of Correlated Information Sources".

V. Ph.D. Dissertations Completed Under Previous AFOSR Contracts

1. "Burst-Error and Random-Error Correction Over q-ary Input, p-ary Output Channels", by Stanley Wainberg - 1972.

2. "Detection/Estimation of Harmonic Sets" by J. D. Patterson - 1972.

3. "Multidimensional Statistical Communication Theory", by Dennis Mangano - 1972.

4. "Studies of Low-Rate Binary Codes", by Anthony Kerdock - 1972.

5. "On the Theory of Confidence Set Estimators and Detection", by P. Donald Hartman - 1972.

6. "The Time Dispersive Channel as a Linear Encoder", by Theodore J. Klein - 1970.

7. "A Study of Lee Metric Codes", by Chung-Yaw Chiang - 1970.

8. "Rate-Distortion Functions for Correlated Gaussian Sources", by Barry J. Bunin - 1970.

9. "Error Bounds for the Binary Input Gaussian Noise Channel with Quantization", by Edward A. Walvick - 1969.

10. "Burst-Error Correction", by John Dewey Bridwell - 1968.

11. "On the Transmission of Information Over the Gaussian and Related Channels", by Leonard Schiff - 1968.

12. "Nonparametric Detection Using Extreme-Value Theory", by Laurence B. Milstein - 1968.

13. "Error Control on Real Channels", by Michael Muntner - 1968.

14. "Some Results for Additive Noise Channels with Noiseless Information Feedback", by Thomas W. Eddy - 1968.

15. "Invariant Estimation of Stochastic Systems Parameters", by Guner Suzek - 1966.

VI. Journal Articles Supported Under Previous AFOSR Contracts

1. N. T. Gaarder and J. K. Wolf, "The Capacity Region of a Multiple-Access Discrete Memoryless Channel Can Increase With Feedback," IEEE Transactions on Information Theory, Vol. IT-21, No. 1, pp. 100-102, January 1975.

2. J. K. Wolf, "Data Reduction for Multiple Correlated Sources," (Invited Paper), Fifth Colloquium on Microwave Communication, pp. ST-287 to ST-295, Budapest, Hungary, June 1074.

3. D. Slepian and J. K. Wolf, "A Coding Theorem for Multiple Access Channels with Correlated Sources," Bell System Technical Journal, pp. 1037-1076, September 1973.

4. J. K. Wolf, "A Survey of Coding Theory: 1967-1972," IEEE Transactions on Information Theory, Vol. IT-19, No. 4, pp. 381-389, July 1973, (Invited Paper).

5. D. Slepian and J. K. Wolf, "Noiseless Coding of Correlated Information Sources," IEEE Transactions on Information Theory, Vol. IT-19, No. 4, pp. 471-480, July 1973.

6. S. Wainberg and J. K. Wolf, "Burst Decoding of Binary Block Codes in Q-ary Output Channels," IEEE Transactions on Information Theory, Vol. IT-18, pp. 684-686, September 1972, (Correspondence).

7. A. M. Kerdock, "A Class of Low Rate Nonlinear Binary Codes," Information and Control, Vol. 20, No. 2, pp. 182-187, March 1972.

8. S. Wainberg and J. K. Wolf, "Algebraic Decoding of Block Codes Over q-ary Input Q-ary Output Channel, Q > q," Information and Control, April 1973.

9. A. Kerdock and J. K. Wolf, "On the Minimum Distortion of Block Codes for a Binary Symmetric Source," IEEE Transactions on Information Theory, Vol. IT-18, pp. 433-435, May 1972, (Correspondence).

10. T. Berger, F. Jelinek and J. K. Wolf, "Permutation Codes for Sources," IEEE Transactions on Information Theory, Vol. IT-18, pp. 160-169, January 1972.

11. J. Ch-Y Chiang and J. K. Wolf, "On Channels and Codes for the Lee Metric," Information and Control, Vol. 19, pp. 159-173, September 1971.

12. T. J. Klein and J. K. Wolf, "On the Use of Channel Introduced Redundancy for Error Correction," IEEE Transactions on Communication Technology, Vol. COM-19, pp. 396-402, August 1971.

13. B. J. Bunin and J. K. Wolf, "Convergence to the Rate-Distortion Function for Gaussian Sources," IEEE Transactions on Information Theory, Vol. IT-17, No. 1, January 1971.

14. S. Wainberg and J. K. Wolf, "Subsequences of Pseudo Random Sequences," IEEE TRansactions on Communication Technology, Vol. COM-18, No. 5, October 1970.

15. J. D. Bridwell and J. K. Wolf, "Burst Distance and Multiple-Burst Correction," Bell System Technical Journal, Vol. 49, pp. 889-909, May-June 1970.

16. B. J. Bunin, "Rate-Distortion Functions for Gaussian Markov Processes," Bell System Technical Journal, Vol. 48, pp. 3059-3074, November 1969.

17. J. K. Wolf, M. L. Shooman and R. R. Boorstyn, "Algebraic Coding and Digital Redundancy," IEEE Transactions on Reliability, Vol. R-18, pp. 91-107, August 1969.

18. J. K. Wolf (with Appendix by R. Graham and J. K. Wolf), "Adding Two Information Symbols to Certain Nonbinary BCH Codes and Some Applications," Bell System Technical Journal, Vol. 48, pp. 2405-2424, September 1969.

19. Laurence B. Milstein, Donald L. Schilling and J. K. Wolf, "Robust Detection Using Extreme-Value Theory," IEEE Transactions on Information Theory, Vol. IT-15, pp. 370-395, May 1969.

20. L. Schiff and J. K. Wolf, "High Speed Binary Data Transmission Over the Additive Band-Limited Gaussian Channel," IEEE Transactions on Information Theory, Vol. IT-15, pp. 287-295, March 1969.

21. L. Schiff, "The Asymptotic Error Probability for Transmission of Orthogonal Signals Over the Generalized Incoherent Channel," IEEE Transactions on Information Theory, Vol. IT-15, pp. 48-52, January 1969.

22. M. Muntner and J. K. Wolf, "Predicted Performance of Error-Control Techniques Over Real Channels," IEEE Transactions on Information Theory, Vol. IT-14, pp. 640-650, September 1968.

23. D. Calabro and J. K. Wolf, "On the Synthesis of Two-Dimensional Arrays with Desirable Correlation Properties," Information and Control, Vol. 11, pp. 537-560, November 1967.

24. B. J. Masnick and J. K. Wolf, "On Linear Unequal Error Protection Codes," IEEE Transactions on Information Theory, Vol. IT-13, No. 4, October 1967.

25. J. K. Wolf, "Decoding of Bose-Choudhuri Codes and Prony's Method of Curve Fitting," IEEE Transactions on Information Theory, Vol. IT-13, No. 4, p. 608, October 1967, (Correspondence).

26. K. Levitt and J. K. Wolf, "A Class of Nonlinear Error Correcting Codes Based Upon Interleaved Two-Level Sequences," IEEE Transactions on Information Theory, Vol. IT-13, pp. 335-336, April 1967.

27. A. I. Liff and J. K. Wolf, "On the Optimum Sampling Rate for Discrete-Time Modeling of Continuous-Time Systems," IEEE Transactions on Automatic Control, Vol. AC-11, pp. 288-290, April 1966.